This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

BIBLIOGRAPHIC RECORD TARGET

Graduate Library
University of Michigan

Preservation Office

Storage Number: _____

ACM0005
UL FMT B RT a BL m T/C DT 07/18/88 R/DT 07/18/88 CC STAT mm E/L 1
010: : |a 22016191
035/1: : |a (RLIN)MIUG86-B24191
035/2: : |a (CaOTULAS)160429583
040: : |c NIC |d NIC |d MiU
050/1:0 : |a QA244 |b .M6
100:1 : |a Mordell, Louis Joel.
245:00: |a Three lectures on Fermat's last theorem, |c by L. J. Mordell.
260: : |a Cambridge [Eng.] |b The University Press, |c 1921.
300/1: : |a 4 p.l., 31, [1] p. |c 22 cm.
650/1: 0: |a Fermat's theorem
998: : |c SMB |s 9124

Scanned by Imagenes Digitales
Nogales, AZ

On behalf of
Preservation Division
The University of Michigan Libraries

Date work Began: _____
Camera Operator: _____

Hosted by Google

THREE LECTURES ON FERMAT'S LAST THEOREM

Hosted by Google

CAMBRIDGE UNIVERSITY PRESS
C. F. CLAY, MANAGER
LONDON : FETTER LANE, E.C. 4

NEW YORK : THE MACMILLAN CO.
BOMBAY
CALCUTTA } MACMILLAN AND CO., LTD.
MADRAS
TORONTO : THE MACMILLAN CO. OF CANADA, LTD.
TOKYO : MARUZEN-KABUSHIKI-KAISHA

ALL RIGHTS RESERVED

Hosted by Google

THREE LECTURES ON FERMAT'S LAST THEOREM

BY

L. J. MORDELL

MANCHESTER COLLEGE OF TECHNOLOGY

CAMBRIDGE
AT THE UNIVERSITY PRESS
1921

Hosted by Google

Hosted by Google

PREFACE

IN March 1920, I gave at Birkbeck College, London, a course of three public lectures on Fermat's Last Theorem. The lectures were intended primarily for persons with a mathematical training, but not necessarily for those who had made a special study of the Theory of Numbers. A general account was given of the various methods that have been devised for dealing with the question, more attention being paid to principles than to details.

This booklet consists of the lectures in practically the form in which they were delivered. It also includes a few details which it was found convenient to omit from the lectures. I hope it may be of assistance in giving to the reader some idea, not only of the difficulties involved, but also of the progress made in dealing with this famous theorem.

I have to acknowledge my indebtedness not only to the authors mentioned herein, but also to the works of Smith, Bachmann, Hilbert, Kronecker, Sommer, and Dickson, on the Theory of Numbers. Full references to the subject are given by Dickson in his very useful paper on "Fermat's Last Theorem" in the *Annals of Mathematics*, Vol. XVIII. 1917 ; and in Vol. II. of his *History of the Theory of Numbers*, which has just been published.

L. J. MORDELL.

November 1920.

Hosted by Google

Hosted by Google

CONTENTS

CHAP.		PAGE
I	. . . . .	1
II	. . . . .	10
III	. . . . .	26

Hosted by Google

Hosted by Google

CHAPTER I

STATEMENT OF THE THEOREM

Of all the abstract sciences, perhaps none is so remarkable for the ease with which theorems are arrived at inductively, and for the difficulty and importance of the developments arising in the efforts to prove the theorems so suggested, as the Theory of Numbers. An admirable illustration of this fact is furnished by Fermat's Last Theorem, namely, that if n is a positive integer greater than two, the equation

$$x^n + y^n = z^n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

cannot be satisfied by integer values for the unknowns x, y, and z unless one of them is zero. On the contrary, when $n = 2$, it is well known that the equation possesses an infinite number of solutions in integers.

Fermat (1601—1665) was a French mathematician of the first rank, who made a special study of the Theory of Numbers, including that part of the subject dealing with the solution of indeterminate equations, called Diophantine Analysis, after the Greek mathematician Diophantus who flourished during* the third century A.D. A new edition of the latter's works was brought out by Bachet in 1621. Fermat possessed a copy of this work and entered in the margin of the pages a number of theorems he had discovered, most of which are now included as special cases in the classical theory of the subject, but without any proofs or indications of his methods. Besides the theorem now known as his last theorem, he placed the remark that he had discovered a truly wonderful proof but that the margin of the book was too small to contain it. Since that time, no general proof has been found for all values of n, even though it has been attempted by the greatest of mathematicians including Euler, Legendre, Gauss, Abel, Dirichlet, Cauchy and Kummer, has been several times made the prize question of learned societies such as the Academies at Paris and Brussels, and though finally, in 1907, a prize of 100,000 marks was established for the first proof.

* *Diophantus of Alexandria*, by Sir Thomas L. Heath, 2nd edition, p. 2.

Hosted by Google

Did Fermat prove his Theorem?

The question immediately suggests itself.—Is it probable, that nearly three centuries ago, Fermat really proved this theorem, which still baffles mathematicians who have at their disposal the wonderful and far reaching developments in mathematics since Fermat's time—especially as it seems likely that Fermat's methods could only be elementary considered from a modern standpoint? From what is known of Fermat's character, it is fairly certain that at any rate he was under the impression that he had a proof meriting his description of it. This statement is confirmed by the fact that when enunciating a theorem to the effect that $2^{2^n}+1$ was a prime number for all positive integral values of n, he added that while convinced of the truth of this theorem, he could not prove it*. Many years afterwards Euler showed that the theorem was false, and that 641 was a factor when $n=5$.

It is of course possible that Fermat was mistaken in thinking that his proof was valid, for even the greatest of mathematicians have made mistakes. The late Prof. H. J. S. Smith, while pointing out that Gauss was unfavourably inclined to Fermat, thought however that there was no ground for supposing that Fermat was mistaken.

Analysis of another statement by Fermat

A little light perhaps may be thrown on Fermat's statement by considering a similar case. He had proposed as a problem to the English mathematicians to show that there was only one integer solution of the equation

$$y^3 = x^2 + 2,$$

obviously $x = \pm 5$, $y = 3$. On this he has a note to the effect that there was no difficulty in finding a solution in fractions, but that he had discovered an entirely new method, wonderfully beautiful and most subtle, which enabled him to solve such questions in integers. This statement seems clear and straightforward and would lead one to suppose that, given an equation of the form

$$y^3 = x^2 + k,$$

where k is an integer, Fermat possessed a method which enabled him to ascertain if the equation possessed integer solutions, and in that case to find them.

* See however Dickson's *History of the Theory of Numbers*, Vol. I. p. 375.

Hosted by Google

Fermat's statement, however, cannot be as clear as it seems to be. For I showed* several years ago that no equation of the form

$$y^3 = x^2 + k,$$

where k is a positive or negative integer, could have more than a finite number of integer solutions. It seems unlikely that this fact was known to Fermat, so we are led to conjecture that his method must have been equivalent to some such process as the following.

In $$y^3 = x^2 + 2,$$

put $$y = a^2 + 2b^2,$$

where a and b are integers, and take

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3.$$

Equating real and imaginary parts

$$x = a^3 - 6ab^2,$$

$$1 = b(3a^2 - 2b^2).$$

Since a and b are integers

$$b = \pm 1, \quad 3a^2 - 2b^2 = \pm 1,$$

or $$b = \pm 1, \quad a = \pm 1,$$

giving $$x = \pm 5, \quad y = 3.$$

It is of course by no means obvious that this process, which can be described without the use of complex quantities, gives all the values of x and y. In any case it seems doubtful if Fermat's description of his method would be justified at the present time.

At the same time it is possible that Fermat did possess a valid proof of his last theorem, but from the circumstances of the case, it is extremely difficult for us to form any conception of his method. One can easily recall a number of theorems which have proved extraordinarily difficult to great mathematicians and which now seem elementary enough. Nothing can appear simpler than the solution of the cubic equation, but many centuries elapsed between the solution of the quadratic and of the cubic. Another instance of a different type is supplied by the proof of the transcendental character of π, i.e. the impossibility of solving the problem commonly called the

* A statement by Fermat, *Proceedings of the London Mathematical Society* (Read Feb. 1918), (Records, etc.), Ser. 2, Vol. XVIII. (1919), pp. v, vi. The same result holds for the equation

$$ey^2 = ax^3 + bx^2 + cx + d,$$

where a, b, c, d, e are any integers for which the right-hand side has no squared factors in x.

Hosted by Google

squaring of the circle, which can now be put in a very simple and elementary form.

Mathematical study and research are very suggestive of mountaineering. Whymper made seven efforts before he climbed the Matterhorn in the 1860's and even then it cost the lives of four of his party. Now, however, any tourist can be hauled up for a small cost, and perhaps does not appreciate the difficulty of the original ascent. So in mathematics, it may be found hard to realise the great initial difficulty of making a little step which now seems so natural and obvious, and it may not be surprising if such a step has been found and lost again.

A SIMPLIFICATION OF THE PROBLEM

Coming back to the equation

$$x^n + y^n = z^n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1),$$

it is obvious that if any two of the unknowns have a common factor k, then the third unknown is also divisible by k. Putting

$$x,\ y,\ z = k\xi,\ k\eta,\ k\zeta,$$

respectively, in equation (1), k^n divides out, leaving

$$\xi^n + \eta^n = \zeta^n,$$

where now no two of the unknowns have a common factor. There will be no loss of generality then if it is supposed that no two of the unknowns in the original equation (1) have a common factor. Next it is sufficient to prove the impossibility of equation (1) when n is equal to 4 or to any odd prime p. For if each of the equations

$$x^4 + y^4 = z^4, \quad x^p + y^p = z^p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

is insoluble, the same holds of equation (1) since n must be divisible by either 4 or an odd prime. For example if n is divisible by p, say $n = pq$, equation (1) can be written as

$$(x^q)^p + (y^q)^p = (z^q)^p,$$

which is then insoluble because of the special case (2).

THE EQUATION $x^2 + y^2 = z^2$

As regards the case $n = 2$, it is well known that the general solution of

$$x^2 + y^2 = z^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3),$$

wherein no two of the unknowns have a common factor, is given by

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

where y is that one of the unknowns which is even, and a and b are prime to each other and not both odd. This result was known to the Indian mathematicians.

Hosted by Google

THE EQUATION $x^4 + y^4 = z^4$

The case $n = 4$ is remarkable not only from the fact that in contradistinction to all the other values of n, the theorem can be rigorously proved by absolutely elementary means, that is by methods which do not implicitly make use of new ideas unknown during Fermat's time, but also from the fact that a proof by Fermat for a very closely related theorem is extant. A proof was given by Leibnitz in a manuscript dated December 1678, and also by Euler.

The proof of the theorem is so simple that it will be worth while giving it completely.

It is obviously sufficient to consider the equation

$$x^4 + y^4 = z^2,$$

where x, y and z are all prime to each other. Further it may be assumed that all the quantities referred to are positive. As all numbers are either odd or even, x is of the form $2m$ or $2m + 1$, where m is an integer. Hence x^2 is of the form $4m^2$ or $4m^2 + 4m + 1$, that is of the form $4M$ or $4M + 1$, so that a number of the form $4M + 2$ or $4M + 3$ cannot be a square. Hence x and y cannot both be odd, for then the sum of their fourth powers would be of the form $4M + 2$, and this cannot be a square. Hence either x or y must be even, and as it is obviously immaterial which one is, suppose it is y. Since

$$(x^2)^2 + (y^2)^2 = z^2,$$

it follows from equation (3) that we must have

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2,$$

where a and b are prime to each other, and not both odd. From

$$x^2 = a^2 - b^2$$

we see that a cannot be even, for then b would be odd and x^2 would be of the form $4M + 3$, which is impossible. We have then

$$x^2 + b^2 = a^2,$$

where b is even, a is odd and prime to b, so that no two of a, b, x have a common factor. Hence it follows from equation (3) that

$$x = p^2 - q^2, \quad b = 2pq, \quad a = p^2 + q^2,$$

where p and q are prime to each other and not both odd. From

$$y^2 = 2ab,$$

we have

$$y^2 = 4pq\,(p^2 + q^2).$$

Hosted by Google

Since p and q are prime to each other, each of them is prime to $p^2 + q^2$, and hence all three must be perfect squares. Put then

$$p = r^2, \quad q = s^2, \quad p^2 + q^2 = t^2,$$

from which
$$r^4 + s^4 = t^2.$$

Now the values of x, y, z in terms of r, s, t are given by

$$x = r^4 - s^4, \quad y = 2rst, \quad z = a^2 + b^2 = r^8 + 6r^4s^4 + s^8,$$

so that
$$z > (r^4 + s^4)^2 > t^4 \quad \text{or} \quad t < \sqrt[4]{z}.$$

It follows then that if one solution of the equation

$$x^4 + y^4 = z^2$$

is known for which none of the unknowns is zero, another solution (r, s, t) can be found for which none of the unknowns is zero and such that $t < \sqrt[4]{z}$. This process can be continued, so that an infinite number of positive integers $t, t_1, t_2 \ldots$ can be found such that

$$t_1 < \sqrt[4]{t}, \quad t_2 < \sqrt[4]{t_1} \ldots,$$

which is clearly absurd.

This proves the impossibility in the case of $n = 4$, the method of proof being known as the method of infinite descent.

THE EQUATION $x^3 + y^3 = z^3$

The case $n = 3$, that is the equation

$$x^3 + y^3 = z^3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4),$$

had been known to the Arabian mathematicians nearly seven hundred years before the time of Fermat, and a faulty proof of the impossibility had been given by them. It is very probable that Fermat discovered this special case before he discovered the general theorem, for he had proposed as a problem "to find values of x, y, and z satisfying the equation," and had later declared it was impossible. Euler was the first to prove the theorem for this special case, but his proof was incomplete in respect of an assumption wherein lay the real difficulty of the question, and which contained the germ of the development of the theory of ideals which was to be applied so successfully by Kummer many years later. Euler's proof as given in his Algebra is substantially as follows.

Two of the unknowns x, y, z must be odd, and as any of the unknowns may be either positive or negative, there is no loss of generality in supposing that z is even, and that x and y are both odd.

Hosted by Google

Write then $x + y = 2p, \quad x - y = 2q$

so that $x = p + q, \quad y = p - q,$

and the original equation becomes

$$2p\,(p^2 + 3q^2) = z^3.$$

Now p and q are prime to each other, and cannot both be odd, for then x and y would not be prime to each other. Further p cannot be odd and q even, for then z^3 would be divisible by 2 and not by 8, which is impossible. Hence p must be even and q odd, so that $p^2 + 3q^2$ is odd. Hence as p and q are prime to each other,

$$2p \text{ and } p^2 + 3q^2$$

are either prime to each other, or have a common factor 3. In the first case p and hence z are both prime to 3, while in the latter case they are both divisible by 3.

Let us consider the first case in detail. As $2p$ and $p^2 + 3q^2$ are prime to each other, each must be a perfect cube, so that we can write

$$p^2 + 3q^2 = r^3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5).$$

Values of p, q, r can be found by taking

$$r = m^2 + 3n^2,$$

where m and n are integers, and writing

$$p + q\sqrt{-3} = (m + n\sqrt{-3})^3.$$

By equating real and imaginary parts

$$p = m^3 - 9mn^2, \quad q = 3m^2n - 3n^3,$$

and if m and n are prime to each other and not both odd, and m is not divisible by 3, then p and q are prime to each other and p is not divisible by 3. But though this method gives suitable values of p, q, r satisfying

$$p^2 + 3q^2 = r^3,$$

it is by no means obvious that all the values of p, q, r can be found in this way, though as a matter of fact it is so in this particular case. If the equation had been

$$p^2 + 11q^2 = r^3,$$

all the values of p and q would not be given by putting

$$p + q\sqrt{-11} = (m + n\sqrt{-11})^3.$$

The removal of the difficulty involves the study of the arithmetical theory of the binary quadratic form, or of ideal numbers.

Hosted by Google

Now since $2p$ is a cube, the values of m and n are such that

$$2m\,(m + 3n)\,(m - 3n)$$

is a perfect cube.

But since $$q = 3n\,(m + n)\,(m - n)$$

is odd, n is odd and m is even. Hence since m is prime to 3, no two of $2m$, $m + 3n$, $m - 3n$ can have a common factor; and since their product is a perfect cube, each of them must be a cube. Put then

$$m + 3n = a^3, \quad m - 3n = b^3, \quad 2m = c^3,$$

so that by addition $$a^3 + b^3 = c^3.$$

Hence $$z^3 = 2p\,(p^2 + 3q^2) = a^3b^3c^3\,(m^2 + 3n^2)^3,$$

or $$z = abc\,(m^2 + 3n^2) = \tfrac{1}{3}abc\,(a^6 + a^3b^3 + b^6),$$

so that as a and b cannot both be unity, z is numerically greater than c. It follows then, just as in the case when $n = 4$, that we should have an infinite sequence of numerically decreasing integers, which is impossible.

The same result follows in the second case when z is divisible by 3, but we need not go into details.

THE EQUATIONS $x^5 + y^5 = z^5$ AND $x^7 + y^7 = z^7$

The next cases to be proved were when $n = 5$ or 7. The first case was dealt with by Legendre and Dirichlet in 1825, while the case of $n = 7$ was proved in 1840 by Lamé and Lebesgue. The proofs involved ideas not greatly dissimilar from the case when $n = 3$ and depended upon two facts. Firstly, that if p is a prime and x and y are prime to each other, the two expressions

$$x + y \text{ and } \frac{x^p + y^p}{x + y}$$

are either prime to each other, or have as a common factor the first power only of p. The proof is immediate, for putting

$$x + y = s,$$

the two expressions become

$$s \text{ and } \frac{x^p + (s - x)^p}{s},$$

or

$$s \text{ and } s^{p-1} - ps^{p-2}x + \frac{p \cdot p-1}{\underline{|2}}\,s^{p-3}x^2 \ldots + \frac{p \cdot p-1}{\underline{|2}}\,sx^{p-2} + px^{p-1}.$$

Also s is prime to x, whence the result, which is due to Jaquemet (1651—1729), follows.

Hosted by Google

The second fact is that $\frac{x^p + y^p}{x + y}$ can be written in the form

$$\tfrac{1}{4}(U^2 - (-1)^{\frac{p-1}{2}} p V^2),$$

where U and V are polynomials in x and y, but the proof is more complicated than that for the first fact so it may be omitted here. In the particular case, however, when $n = 5$ or 7, there is no difficulty in finding U and V by elementary algebra.

Taking now the case $n = 5$, we have

$$z^5 = (x + y)\left(\frac{x^5 + y^5}{x + y}\right),$$

or

$$z^5 = (x + y)\left(\frac{U^2 - 5V^2}{4}\right),$$

where U and V are quadratic functions of x and y. From the above, the two factors on the right-hand side are either prime to each other, or have a common factor 5 of which the first power only will divide $\frac{U^2 - 5V^2}{4}$. We then have an equation of the form

$$\tfrac{1}{4}(U^2 - 5V^2) = W^5 \text{ or } 5W^5.$$

The difficulty arising in the case $n = 3$, and overlooked by Euler, occurs in the discussion of these equations, but it is possible to avoid it by similar methods. It follows also that the case $n = 5$ is impossible. A similar method applies to the case $n = 7$, but more algebra is required than for $n = 5$.

Hosted by Google

CHAPTER II

KUMMER'S WORK

The difficulties arising with increasing values of n soon made it clear that other methods were required for the general case. These, of which we shall now give an account, were introduced by Kummer (1810—1893). His results were the most important contribution to this subject by any mathematician either before or after his time. Not only were they the most general, in that he succeeded in proving Fermat's Last Theorem for a large number of values of n included in several classes, but they were also the most useful, and marked an important stage in the development of mathematics. The theory of ideals, which is now part of the fundamental groundwork of the Theory of Numbers, had its origin in Kummer's researches on this subject and the general law of reciprocity. His methods and results were the starting point of numerous investigations commenced many years after his time, and have led to some very surprising results even within the last twelve years. His work is an excellent illustration of the great indebtedness of mathematics and mathematicians to the consideration of one or two isolated questions.

Writing the equation (p an odd prime)

$$x^p + y^p = z^p$$

in the form

$$(x+y)(x+\zeta y)(x+\zeta^2 y) \ldots (x+\zeta^{p-1} y) = z^p \quad \ldots\ldots\ldots(6),$$

where ζ is a complex pth root of unity, the attention of mathematicians was drawn to the study of expressions of the form

$$a + b\zeta + c\zeta^2 + \ldots k\zeta^{p-1},$$

where $a, b, c \ldots$ are integers, and to inquire if the ordinary laws of arithmetic applied to such expressions.

Many of the most important developments of arithmetic depend upon the definition of a prime number and the so called factor theorem, namely that every number can be resolved into prime factors in one way only. It follows from this fact that if positive integers $A, B, C \ldots K, L$, of which no two have a common factor, satisfy the condition

$$ABC \ldots K = L^p,$$

Hosted by Google

then each of the numbers A, $B \ldots K$ must be a perfect pth power. Should any of the quantities A, $B \ldots$ have a common factor, this result must be slightly modified; for example A now will be a perfect pth power multiplied by a constant depending on the common factors mentioned above. Particular cases of this theorem have already been used. The question immediately suggests itself—Can this theorem be extended to apply to equation (6), and can we deduce that the factors $x + \zeta y$, $x + \zeta^2 y \ldots$ are each pth powers of expressions of the form

$$a + b\zeta + c\zeta^2 + \ldots$$

or perhaps multiples of such pth powers? If so, a proof of Fermat's Last Theorem would be fairly easy.

Arithmetical properties of numbers of the form $a + ib$

Before we answer this question, let us consider what occurs in some analogous but simpler cases. The simplest case would be the study of complex numbers of the form

$$a + ib,$$

where $i = \sqrt{-1}$ and a and b are rational numbers. When a and b are integers it seems natural to call the complex number $a + ib$ a complex integer. When $b = 0$ the complex integer becomes an ordinary integer. Further it is obvious that the sum, difference or product of two complex integers is also a complex integer, so that the definition of a complex integer is consistent.

As regards division, a complex integer $a + ib$ is said to be divisible by a complex integer $c + id$ if a complex integer $x + iy$ can be found so that

$$a + ib = (c + id)(x + iy).$$

We note that while 1 is exactly divisible by only two integers, namely ± 1, it is exactly divisible by four integers in the complex theory, namely ± 1, $\pm i$. The divisors of unity are called units.

The question now arises, "What is the definition of a prime number in the new theory?" The odd primes

$$3,\ 5,\ 7,\ 11,\ 13,\ 17, \ldots$$

can be divided into two groups such as

$$5,\ 13,\ 17,\ 29,\ 37, \ldots$$

of which every one leaves the remainder 1 when divided by 4; and

$$3,\ 7,\ 11,\ 19, \ldots$$

every one of which leaves the remainder 3 when divided by 4.

Hosted by Google

The numbers in the first group, however, are no longer primes in the complex theory. For it is clear that

$$5 = (2+i)(2-i),$$
$$13 = (3+2i)(3-2i),$$
$$17 = (4+i)(4-i),$$

and it can be shown that every prime number of the form $4n+1$ can be expressed in this way, that is

$$4n+1 = (a+ib)(a-ib) = a^2+b^2,$$

where a and b are integers. This fact was indeed stated by Fermat and first proved by Euler, but it is of an entirely different kind from the theorems of elementary arithmetic.

The numbers in the second group cannot be factorised in this way, for then

$$4n+3 = (a+ib)(a-ib) = a^2+b^2.$$

But as already remarked, the square of any integer when divided by 4 leaves a remainder 0 or 1. Hence a^2+b^2 when divided by 4 can only leave a remainder 0, 1, 2 and not 3. This proves the statement.

The behaviour of the even prime 2 is very different from that of the odd primes. For

$$2 = i(1-i)^2,$$

so that 2 is practically* a square number in the complex theory.

We can now define the prime numbers of the complex theory. These are the numbers

$$3,\ 7,\ 11,\ 19, \ldots,$$

that is the primes of the form $4n+3$ in the ordinary theory; the complex quantities

$$2 \pm i, \quad 3 \pm 2i \ldots a \pm ib,$$

which are the factors of 5, 13, ... and of the primes of the form $4n+1$; and lastly $1-i$.

THE FACTOR THEOREM FOR PRIMES IN THE NEW THEORY

It can be shown that in the complex theory, the primes, as just defined, have properties practically identical with those of the ordinary primes. For example every complex integer can be resolved into prime factors in one way and only one way, noting of course that the factors

$$a+ib, \quad -(a+ib), \quad \pm(a+ib)$$

are not considered as different.

* That is, except for the unit factor i.

Hosted by Google

Suppose for instance that $a + ib$ is a factor of the number p which is a prime in the ordinary theory, so that

$$a^2 + b^2 = p.$$

Then $x + iy$ is divisible by $a + ib$ if

$$\frac{x + iy}{a + ib} = \frac{(x + iy)(a - ib)}{a^2 + b^2}$$

is a complex integer. Hence

$$\xi = ax + by \quad \text{and} \quad \eta = ay - bx$$

must both be divisible by p. But as

$$a\xi - b\eta = (a^2 + b^2)\, x = px,$$

and a and b are both prime to p, it is clear that ξ and η are both divisible by p if one of them is. Hence the condition that*

$$(x_1 + iy_1)(x_2 + iy_2) \equiv 0 \pmod{(a + ib)},$$

is that $$b(x_1x_2 - y_1y_2) - a(x_1y_2 + x_2y_1) \equiv 0 \pmod{p},$$

or multiplying by b

$$b^2(x_1x_2 - y_1y_2) - ab(x_1y_2 + x_2y_1) \equiv 0 \pmod{p},$$

which since $$a^2 + b^2 \equiv 0 \pmod{p},$$

can be written as

$$(ay_1 - bx_1)(ay_2 - bx_2) \equiv 0 \pmod{p}.$$

Hence one of these two factors must be divisible by p, that is, the corresponding factor $x_1 + iy_1$ or $x_2 + iy_2$ is divisible by p. This shows that practically the same arithmetical laws hold for complex integers as for ordinary ones.

THE EQUATION $x^2 + y^2 = z^n$

We can now solve the equation

$$x^2 + y^2 = z^n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6\,a),$$

where x, y and z are ordinary integers no two of which have a common factor, by writing

$$(x + iy)(x - iy) = z^n.$$

Now in the complex theory x and y are still prime to each other, so that the common factor of the two complex quantities $x + iy$, $x - iy$ must be a divisor of 2, that is the common factor must be 1, $1 + i$ or 2. We can exclude 2 because then x and y would both be even.

We can also exclude $1 + i$, for if

$$\frac{x + iy}{1 + i} = \frac{x + y + i(y - x)}{2}$$

* The statement $A \equiv B \pmod{C}$ means that $A - B$ is divisible by C.

Hosted by Google

were a complex integer, $x+y$ and $x-y$ would both be divisible by 2, or since x and y are both prime to each other, this means that x and y are both odd. But this is impossible for then x^2+y^2 would be double an odd number and could not be a perfect nth power if $n>1$. Hence as $x+iy$ and $x-iy$ are prime to each other, each of them, except for a unit factor, must be a perfect nth power, so that the solution of the equation (6 a) is given by

$$x+iy=i^r(a+ib)^n, \qquad x-iy=i^{-r}(a-ib)^n,$$
$$z=a^2+b^2,$$

where a and b are ordinary integers such that x, y and z have no common factor, and r is any integer.

Numbers of other kinds, and their factorisation

The difficulties arising then in the discussion of complex integers of the type $a+ib$ are comparatively simple. These complex integers naturally suggest algebraic integers of a more general type, such as for example, $a+b\sqrt{m}$, where a, b and m are rational quantities. We shall consider in particular the study of the quantities $x=a+b\sqrt{-5}$, where a and b are rational, and shall call x an algebraic integer if a and b are integers. A more general definition is that x is an algebraic integer if it is a root of an algebraic equation of which the coefficients are integers, while the coefficient of the highest power of x is unity. The two definitions are equivalent in our special case, though they would not be so if $\sqrt{-5}$ were replaced by $\sqrt{5}$. The addition, subtraction, division or multiplication of such integers calls for no comment. It is when we start to factorise such algebraic integers that a difficulty soon arises. It seems natural to call an algebraic integer $x+y\sqrt{-5}$ a prime when it is not divisible by $a+b\sqrt{-5}$ unless $a=\pm x$, $b=\pm y$. Let us accept this definition of a prime.

Take the number 21 for example. Clearly we have

$$21=3\times 7=(4+\sqrt{-5})(4-\sqrt{-5})=(1+2\sqrt{-5})(1-2\sqrt{-5}).$$

But $4+\sqrt{-5}$ cannot be resolved into a product of factors of algebraic integers of the form $a+b\sqrt{-5}$. For if this were possible, then

$$4+\sqrt{-5}=(a+b\sqrt{-5})(c+d\sqrt{-5}),$$

say, so that $\qquad 4-\sqrt{-5}=(a-b\sqrt{-5})(c-d\sqrt{-5}).$

Hence by multiplication

$$21=(a^2+5b^2)(c^2+5d^2),$$

Hosted by Google

so that a^2+5b^2, being a factor of 21, must be either 1, 3, 7 or 21. This gives $a=\pm 1$, $b=0$; or $a=\pm 4$, $b=\pm 1$; or $a=\pm 1$, $b=\pm 2$. The solution $a=\pm 1$, $b=0$ does not give a factor of $4+\sqrt{-5}$, while the solution $a=\pm 4$, $b=\pm 1$ does not give a factor, since

$$\frac{4+\sqrt{-5}}{4-\sqrt{-5}}=\frac{11+8\sqrt{-5}}{21}$$

is not a complex integer. It is also easily seen that $\pm 1\pm 2\sqrt{-5}$ is not a factor.

In the same way it is found that neither $1+2\sqrt{-5}$, 3 nor 7 splits into factors of the form $a+b\sqrt{-5}$. We have then 21 expressed as a product of primes in three different ways. Moreover

$$(4+\sqrt{-5})(4-\sqrt{-5}) \text{ is divisible by } 3,$$

where 3 is a prime in the new theory, while $4+\sqrt{-5}$ and $4-\sqrt{-5}$ are both prime to 3. Hence the factor theorem of arithmetic which states that the product of two integers ab cannot be divisible by a prime p, unless either a or b is divisible by p, no longer applies. This breaking down of one of the fundamental laws of arithmetic for integers of the type $a+b\sqrt{-5}$ brings us face to face with a great difficulty, and suggests that the method of defining a prime in the present instance, in the same manner as for integers of the form $a+ib$, is not satisfactory. It is however not obvious at first sight how to suggest an alternative method. Unless this is done, we cannot deduce from the equation $xy=z^2$, where x and y are prime to each other, that x and y are both perfect squares.

For example $(2+\sqrt{-5})(2-\sqrt{-5})=9$,

where the factors $2\pm\sqrt{-5}$ are primes, have no common factor, and are not equal to the squares of integers of the form $a+b\sqrt{-5}$.

The difficulty arising in the general equation

It is now clear that given an equation of the form

$$(x+y)(x+\zeta y)(x+\zeta^2 y)\ldots(x+\zeta^{p-1}y)=z^p \quad \ldots\ldots\ldots(6),$$

where ζ is a complex pth root of unity, it cannot be asserted that $x+\zeta y$, for example, is the pth power of an expression of the form

$$a+b\zeta+c\zeta^2+\ldots k\zeta^{p-1},$$

until an investigation has been made of the arithmetical properties of such algebraic integers. It may happen that the definition of a prime in the new theory in the same way as for numbers of the form $a+ib$

Hosted by Google

will be satisfactory, in which case the algebraic integers can be factorised in one way only; or the same difficulty may arise as in the case of numbers of the form $a + b\sqrt{-5}$. As a matter of fact, it is not true that the algebraic numbers above can be factorised uniquely, but the first case of failure occurs when $p = 23$. It is not surprising then that such mathematicians as Lamé, Cauchy and even Kummer should have been originally under the impression that the algebraic integers above could be factorised uniquely.

Lamé made this false assumption in giving a proof of Fermat's Last Theorem, as was pointed out by Liouville and Kummer. Kummer also had previously made the same mistake in attempting a proof, as was pointed out by Dirichlet, who expressed his belief that the algebraic numbers involved could not in general be factorised uniquely.

The question before us, then, is the removal of the difficulty mentioned above, and a very simple illustration due to Hilbert may show us how this can be done. Let us consider only the odd integers of the form $4n + 1$, that is to say 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69 ..., and investigate what happens when we attempt to build up the arithmetical laws for this group of integers, say a, b, c .... A number a will now be called a prime if it cannot be expressed in the form $a = bc$ unless b or c equals unity. Thus 21 would be a prime number in the new theory, for although

$$21 = 3 \times 7,$$

neither 3 nor 7 is included in the group of integers of the form $4n + 1$. Also $49 \times 9 = 21^2$, and neither 9 nor 49 is the square of a number of the group, while 9 and 49 are prime to each other, since no number* of the group divides both of them. Again 693 can be factorised as

$$693 = 9 \times 77 = 21 \times 33,$$

that is in two essentially different ways, since 9, 21, 33 and 77 must be considered as primes in the new theory.

The difficulties arising now are of exactly the same kind as arose in the consideration of algebraic numbers of the form $a + b\sqrt{-5}$. But the way out of the difficulty is obvious in the present case. Instead of considering only the integers 1, 5, 9, 13 ..., we consider in addition the odd numbers of the form $4n + 3$, for example 3, 7, 11 .... Then we know that in the new group of integers, 1, 3, 5, 7, 9 ..., the ordinary laws of arithmetic hold, and now

$$9 = 3^2, \quad 77 = 7 \times 11, \quad 21 = 3 \times 7, \quad 33 = 3 \times 11,$$

* Except unity.

Hosted by Google

so that the two different methods of factorising 693 reduce to the one way

$$693 = 3^2 \times 7 \times 11.$$

This method of removing the difficulty is very simple and general, and suggests at once the question—Can this idea be extended to the algebraic numbers of the form $a + b\sqrt{-5}$; or in other words can the group of algebraic numbers of the form $a + b\sqrt{-5}$ be enlarged by joining a new group of numbers, so that the factor law of arithmetic holds for this enlarged group? The answer is in the affirmative, not only for these special algebraic numbers, but for all algebraic numbers. The method of doing this has been presented in three different ways* by Kummer†, Dedekind, Kronecker and Weber. The principles underlying them are essentially the same, and are now included under what is known as the arithmetical theory of algebraic numbers.

Introduction of ideal numbers

The methods may be made clearer if presented in a rather different way from those of the investigators above, but which, though very useful for giving a clear insight into the matter, would prove rather difficult if made the starting point of an investigation for the general algebraic number.

For our purpose it may be sufficient to say that instead of considering algebraic numbers of the form $a + b\sqrt{-5}$ we consider the new group of numbers defined by τ, where

$$\tau^2 = x + y\sqrt{-5},$$

and x and y are any integers, whose greatest common factor is a perfect square or 5 times a perfect square, and satisfying the condition that

$$x^2 + 5y^2$$

should be a perfect square. The group of algebraic integers now arising reproduces itself by multiplication and its members may be called ideal numbers. It includes as part of itself the numbers of the form $a + b\sqrt{-5}$, of which we have already spoken.

The ordinary primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 ...

can now be divided into three classes, while 5 is in a class by itself.

* See Bachmann, *Zahlentheorie*, Vol. v. p. 521, for two other methods by Hensel and Sochotzki.

† Kummer dealt only with the algebraic numbers arising from the complex roots of unity.

Hosted by Google

The first class consists of primes such as 29, 41, 61 ..., which can be written in the form

$$29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}),$$
$$41 = (6 + \sqrt{-5})(6 - \sqrt{-5}),$$
$$61 = (4 + 3\sqrt{-5})(4 - 3\sqrt{-5}),$$

that is, each of them can be expressed in the form $a^2 + 5b^2$.

The second class consists of primes such as 3, 7, 23 ..., which cannot be expressed in the form $a^2 + 5b^2$, though their squares can be expressed in this form, for example

$$3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$
$$7^2 = (2 + 3\sqrt{-5})(2 - 3\sqrt{-5}),$$

and in general for any prime p of this kind

$$p^2 = c^2 + 5d^2,$$

or if ideal numbers τ_1, τ_2 are defined by

$$\tau_1^2 = c + d\sqrt{-5}, \quad \tau_2^2 = c - d\sqrt{-5},$$

then p can be factorised in the form

$$p = \tau_1 \tau_2.$$

The third class of primes consists of primes, say q, such as

$$2, 11, 13, 17 \ldots,$$

which are such that neither they nor their squares can be expressed* in the form $a^2 + 5b^2$. A very simple rule enables us to distinguish between the three classes of primes, but the principles employed depend upon the Theory of Numbers. The prime 5 as already remarked is in a class by itself and since $5 = -(\sqrt{-5})^2$, 5 is practically a square number.

The proof of a unique factorisation law

It can be shown that the new group of algebraic integers of the type specified by $\tau = \sqrt{x + y\sqrt{-5}}$, and which includes the complex numbers of the form $m + n\sqrt{-5}$ as a special case, can be factorised uniquely by means of the quantities just denoted by $a + b\sqrt{-5}$, $\sqrt{c + d\sqrt{-5}}$, q and $\sqrt{-5}$.

This follows from the condition of divisibility of an ideal number by the new primes, just as in the case of complex numbers of the form $x + iy$. For example, if the ideal number $\sqrt{x + y\sqrt{-5}}$ is divisible by $\sqrt{2 + \sqrt{-5}}$ say τ, so that τ is an ideal factor of 3, we must have

$$\sqrt{x + y\sqrt{-5}} = \sqrt{2 + \sqrt{-5}}\sqrt{m + n\sqrt{-5}},$$

* We assume that $b \neq 0$.

Hosted by Google

where m and n are integers. It is easily seen that

$$9m = 2x + 5y, \quad 9n = -x + 2y,$$

and that both m and n are integers if

$$x - 2y \equiv 0 \pmod 9.$$

Similarly the number $x + y\sqrt{-5}$ is divisible by τ if

$$\sqrt{x^2 - 5y^2 + 2xy\sqrt{-5}} \text{ is divisible by } \tau.$$

The condition for this is that

$$x^2 - 5y^2 - 4xy \equiv 0 \pmod 9,$$

that is
$$(x - 2y)^2 \equiv 0 \pmod 9,$$

or
$$x - 2y \equiv 0 \pmod 3.$$

We can now prove that if the product of two algebraic numbers is divisible by τ, one of them is divisible by τ. Let the numbers be

$$x_1 + y_1\sqrt{-5}, \quad x_2 + y_2\sqrt{-5}.$$

Their product

$$x_1x_2 - 5y_1y_2 + \sqrt{-5}\,(x_1y_2 + x_2y_1)$$

being divisible by τ, we must have

$$x_1x_2 - 5y_1y_2 - 2\,(x_1y_2 + x_2y_1) \equiv 0 \pmod 3,$$

that is
$$(x_1 - 2y_1)(x_2 - 2y_2) \equiv 0 \pmod 3.$$

This means that one of these two factors must be divisible by 3, so that, if say,

$$x_1 - 2y_1 \equiv 0 \pmod 3,$$

then from the above $x_1 + y_1\sqrt{-5}$ must be divisible by τ.

The same result follows if we consider the product of two ideal numbers $\sqrt{x_1 + y_1\sqrt{-5}}$, $\sqrt{x_2 + y_2\sqrt{-5}}$. This product is divisible by τ if

$$x_1x_2 - 5y_1y_2 - 2\,(x_1y_2 + x_2y_1) \equiv 0 \pmod 9,$$

or
$$(x_1 - 2y_1)(x_2 - 2y_2) \equiv 0 \pmod 9,$$

and a simple discussion shows that if $x_1 - 2y_1$ is divisible by 3, it is also divisible by 9 (noting that $x_1^2 + 5y_1^2$ is a square). Hence as before one of the ideal numbers must be divisible by τ.

It is clear now that being given an algebraic number $x + y\sqrt{-5}$, the condition

$$x - 2y \equiv 0 \pmod 3$$

is sufficient to define the ideal prime factor $\sqrt{2 + \sqrt{-5}}$ of the complex number, and that the actual form of the ideal number need not be

Hosted by Google

given explicitly. Dedekind, for example, put $x - 2y = 3m$, so that $x + y\sqrt{-5}$ becomes $3m + y(2 + \sqrt{-5})$, and then considered the properties of the groups of numbers arising by taking different values for m and y, and called the group of numbers an ideal. Kronecker however would have studied the linear expression as a function of x, y; while Kummer would have used the congruence

$$x - 2y \equiv 0 \pmod 3$$

as defining the ideal prime τ.

Application of ideal numbers to Fermat's Last Theorem

For algebraic numbers of the form

$$a + b\zeta + c\zeta^2 + \ldots$$

Kummer showed that the ideal numbers were of the form

$$\sqrt[r]{a_1 + b_1\zeta + c_1\zeta^2 \ldots},$$

where a_1, b_1, c_1, ... are integers satisfying certain conditions, while r is a factor of a number called the number of ideal classes. Its value depends only on p, and can be found by a very complicated method depending on principles introduced into analysis by Dirichlet.

Continuing now the discussion of the equation

$$(x + y)(x + \zeta y) \ldots (x + \zeta^{p-1} y) = z^p \quad \ldots\ldots\ldots\ldots\ldots (6),$$

consider first the case when z is prime to p. This is tantamount to saying that no two of the factors on the left-hand side have a common factor. Hence by introducing ideal numbers, we have, practically as in the case of the equation $x^2 + y^2 = z^m$, a number of equations of the form

$$x + \zeta y = \xi\tau^p,$$
$$x + \zeta^2 y = \xi_2\tau_2^p,$$
$$\ldots\ldots\ldots\ldots$$

where τ, τ_2, ... are ideal numbers and ξ, ξ_2, ... are units, i.e. quantities of the form

$$a_2 + b_2\zeta + c_2\zeta^2 \ldots,$$

which are divisors of unity.

Noting now the explicit expression for τ, namely

$$\tau = \sqrt[r]{a + b\zeta + c\zeta^2 \ldots},$$

we have

$$x + \zeta y = \xi\,(\sqrt[r]{a + b\zeta + c\zeta^2 \ldots})^p.$$

If now r is prime to p, and this is an extremely important condition, it follows that

$$a + b\zeta + c\zeta^2 \ldots$$

Hosted by Google

is the rth power of a similar expression, so that we can write

$$x + \zeta y = \xi (\alpha + \beta\zeta + \gamma\zeta^2 \ldots)^p,$$

where $\alpha, \beta, \gamma, \ldots$ are integers. We find other equations by changing ζ into $\zeta^2, \zeta^3, \ldots$. It is then a comparatively simple matter to show that equations of this kind are impossible, not only when x and y are ordinary integers but also when they are integers of the form

$$A + B\zeta + C\zeta^2 + \ldots.$$

A similar conclusion can be drawn in the case when z is not prime to p. Hence Fermat's Last Theorem is proved in all the cases where r or the number of classes of ideals is prime to p. The condition for this can be stated in a remarkable form by noting the following expansion in ascending powers of x, namely

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{B_n x^{2n}}{(2n)!},$$

so that $B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$, ... are the well known Bernoulli's numbers. Then the required condition is that the numerators of none of the first $\frac{1}{2}(p-3)$ of the Bernoulli's numbers should be divisible by p. The only primes less than 100 for which this condition is not satisfied are $p = 37, 59, 67$, and hence it is proved* that

$$x^p + y^p = z^p$$

is impossible if p is an odd prime less than 100, except when $p = 37, 59, 67$.

In order to establish the truth of the theorem for these exceptional values of p, Kummer gave in 1857 some additional results for primes satisfying certain conditions†. These conditions were satisfied by $p = 37, 59, 67$, so that Fermat's Last Theorem is proved for *all* values of p, prime or otherwise, less than 100, omitting of course $p = 2$.

Another result by Kummer

Some other important consequences were deduced by Kummer in the special case when one of the unknowns is not divisible by p. We

* A complete account of Kummer's theory of ideal numbers is given in *Liouville's Journal*, t. XVI. 1851. Hilbert in his well known report on "Die Theorie der algebraischen Zahlkörper" gives the modern version. The French translation of this report has an appendix giving other results on Fermat's Last Theorem. For a good introduction, see Sommer, *Vorlesungen über Zahlentheorie*.

† It appears that Kummer has made some errors which vitiate his proof for the cases $p = 37, 59, 67$. See Vandiver "On Kummer's memoir of 1857 concerning Fermat's Last Theorem," *Proceedings of the National Academy of Science, Washington, U.S.A.*, Vol. VI. May, 1920. The case $p = 37$, however, was proved impossible by Mirimanoff in 1892, so that the cases $p = 59, 67$ are still doubtful.

Hosted by Google

saw previously that we could deduce from equation (6) a series of equations of the form

$$x + \zeta^r y = \xi_r \tau_r^p,$$

where $r = 1, 2, \ldots p$. Kummer showed that it was possible to select $\frac{p-1}{2}$ of these equations in such a way that the product of the corresponding τ_r's is an actual number of the form

$$T = a + b\zeta + c\zeta^2 + \ldots.$$

By multiplying together the product of the $\frac{p-1}{2}$ equations, he obtained a result of the form

$$\Pi(x + \zeta^r y) = \pm \zeta^k T^p,$$

where the multiplication on the left refers to the selected $\frac{p-1}{2}$ factors. Replacing ζ by e^v, we have an identity of the form

$$\Pi(x + e^{rv} y) = \pm e^{kv}(a + be^v + \ldots)^p + (1 + e^v + e^{2v} + \ldots e^{(p-1)v}) f(v),$$

where $f(v)$ is a polynomial in e^v with integral coefficients. By differentiation he deduced* that

$$B_n \frac{d^{p-2n}}{dv^{p-2n}} [\mathrm{Log}(x + e^v y)]_{v=0} \equiv 0 \pmod{p},$$

when $n = 1, 2, \ldots \frac{1}{2}(p-3)$, where B_n is the nth Bernoullian number as defined before, a result which has since proved very useful.

Kummer, although not a candidate for a prize offered by the French Academy for a proof of Fermat's Last Theorem, was awarded it in recognition of his researches on complex numbers. Certainly never was an investigator on these subjects more worthy of one.

Deductions from Kummer's last result

For about fifty years after Kummer's work, very little was accomplished either in extending or in developing the full consequences of his results on Fermat's Last Theorem. In the early part of this century, however, mathematicians turned once more to Kummer's results, and in particular to the one, that if

$$x^p + y^p = z^p$$

had solutions for which z is prime to p, then

$$B_n \frac{d^{p-2n}}{dv^{p-2n}} [\mathrm{Log}(x + e^v y)]_{v=0} \equiv 0 \pmod{p}$$

for $n = 1, 2, 3, \ldots \frac{1}{2}(p-3)$.

* *Abhand. Ak. Wiss. Berlin*, 1857.

Hosted by Google

This result, by putting

$$p - 2n = i,$$

can be written in the slightly different form

$$B_{\frac{1}{2}(p-i)} \frac{d^i}{dv^i} [\mathrm{Log}\,(x + e^v y)]_{v=0} \equiv 0 \pmod{p} \quad \ldots\ldots\ldots(7),$$

where $$i = 3,\ 5,\ \ldots\ p-4,\ p-2.$$

Take now $i = 3$, then

$$B_{\frac{1}{2}(p-3)} \frac{d^3}{dv^3} [\mathrm{Log}\,(x + e^v y)]_{v=0} \equiv 0 \pmod{p},$$

and this reduces to

$$B_{\frac{1}{2}(p-3)}\, xy\,(x-y) \equiv 0 \pmod{p}.$$

Hence if $B_{\frac{1}{2}(p-3)}$ is not divisible by p,

$$xy\,(x-y) \equiv 0 \pmod{p}.$$

If then the equation has a solution for which x, y, z are all prime to p,

$$x \equiv y \pmod{p};$$

and in exactly the same way

$$x \equiv z \pmod{p}.$$

This gives $$3x^p \equiv 0 \pmod{p},$$

which is impossible if p is not equal to 3.

Hence we have proved the result that the equation

$$x^p + y^p = z^p$$

cannot have integer solutions for which x, y and z are all prime to p unless $B_{\frac{1}{2}(p-3)}$ is divisible by p. In the same way, by taking $i = 5,\ 7,\ 9$, it is found that in addition

$$B_{\frac{1}{2}(p-5)},\quad B_{\frac{1}{2}(p-7)},\quad B_{\frac{1}{2}(p-9)}$$

must be divisible by p. This was proved by Mirimanoff in 1905, for the last two of the four Bernoulli's numbers above, and by Kummer for the first two, but the case for $B_{\frac{1}{2}(p-3)}$ had been practically announced previously by Cauchy, although without proof.

Mirimanoff also showed by developing the value of

$$\frac{d^i}{dv^i} [\mathrm{Log}\,(x + e^v y)]_{v=0},$$

that, if x, y, z are all prime to p, then Kummer's result (7) could be expressed in the form*

$$B_{\frac{1}{2}(p-i)} (t - 2^{i-1} t^2 + 3^{i-1} t^3 \ldots \pm (p-1)^{i-1} t^{p-1}) \equiv 0 \pmod{p},$$

* *Crelle's Journal*, Vol. CXXVIII.

Hosted by Google

or say $$B_{\frac{1}{2}(p-i)}\, \phi_i(t) \equiv 0 \pmod{p},$$

where $$i = 3,\ 5,\ \ldots\ p-2,$$

and t is the ratio of any pair of x, y, z. Or again in the form

$$\phi_n(t)\, \phi_{p-n}(t) \equiv 0 \pmod{p}$$

where $$n = 1,\ 2,\ \ldots\ p-1.$$

THE CONGRUENCES $2^{p-1} \equiv 1 \pmod{p^2}$, $3^{p-1} \equiv 1 \pmod{p^2}$ ....

A number of conditions can be found by eliminating t from the above congruences. Although there seems no *a priori* reason for expecting simple results, Wieferich* showed in 1909 that one of these conditions could be expressed in the surprisingly simple form

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

This extremely simple and unexpected result represented the first real advance made in the subject since Kummer's work. The Göttingen Academy of Science awarded him 100 marks from the interest of the Wolfskell fund.

In 1913, Meissner showed that $p = 1093$ was the only prime less than 2000 for which this congruence was satisfied.

In other words the equation (p a prime)

$$x^p + y^p = z^p,$$

where $$2000 > p > 2,$$

cannot be satisfied by values of x, y and z, each of which is prime to p, except perhaps when $p = 1093$.

Simpler proofs of Wieferich's result were soon given by Frobenius and Mirimanoff, the latter also showing† that under the same conditions

$$3^{p-1} \equiv 1 \pmod{p^2}.$$

The two congruences above could not of course have been foreseen from Kummer's original results, but another proof was given by Furtwängler, which seems more natural and simple, depending upon ideas which should be capable of further extension. The following may perhaps give some indication of the ideas involved.

Suppose we have two odd primes, say 3 and 7, and it is required to investigate if integers x and y can be found so that

$$x^2 \equiv 7 \pmod{3}, \quad y^2 \equiv 3 \pmod{7}.$$

* *Crelle's Journal*, Vol. CXXXVI.

† *Crelle's Journal*, Vol. CXXXIX.

Hosted by Google

It is easy to see that the first congruence is satisfied by $x = 2$, while the second congruence is impossible. If however 3 and 7 had been replaced by any odd two primes p and q, a very simple theorem known as the law of quadratic reciprocity enables us from the known possibility or impossibility of one of the congruences to determine if the other congruence is possible or not. But if one of the congruences is impossible, we can at once conclude that the equation

$$x^2 = py^2 + qz^2$$

is also impossible.

This theorem, moreover, can be extended to congruences of the form

$$x^p \equiv P \pmod{Q},$$

where x, P, Q are algebraic numbers of the form

$$a + b\zeta + c\zeta^2 + \ldots,$$

or even ideal numbers occurring in the theory of such algebraic numbers. The theorem in this case, known as the general law of reciprocity, was enunciated and proved by Kummer, but only a special case, due to Eisenstein, was required in Furtwängler's* proof. Assuming this result, Furtwängler's proof of the results

$$2^{p-1} \equiv 3^{p-1} \equiv 1 \pmod{p^2}$$

is very simple and natural. As already remarked, it seems that a new application of the laws of reciprocity may be expected to lead to interesting results.

It appears probable that the 2 and 3 above can be replaced by any prime q (except p). In 1914, Vandiver† showed that 5 was another value for q, while Frobenius‡ showed that q might also take the values 11 and 17; and also the values 7, 13, 19, if $p \equiv 5 \pmod{6}$.

The proofs, however, are very complicated and depend upon a special study of the properties of Bernoulli's numbers. The elimination is carried out by taking the congruence

$$B_{\frac{1}{2}(p-i)}\, \phi_i(t) \equiv 0 \pmod{p},$$

multiplying throughout by an appropriate function of t, say $f_i(t)$, and then adding together the left-hand sides of the congruences, which then reduce practically to the form

$$q^{p-1} \equiv 1 \pmod{p^2},$$

for the values $q = 2, 3, 5 \ldots$ as just noted.

* *Sitzungs. Ak. Wiss. Wien* (Math.), Vol. CXXI. 1912 II *a*, pp. 589—592.

† *Crelle's Journal*, Vol. CXLIV. 1914, p. 314.

‡ *Sitzungs. Ak. Wiss. Berlin*, 1914, p. 653.

Hosted by Google

CHAPTER III

LIBRI'S RESULT

We shall now pass on to other methods* which have been employed. These, although of interest, do not prove the truth of Fermat's Last Theorem for even one case.

A simple method of attempting to prove the Theorem, which soon suggests itself to investigators, may be explained by taking the particular case

$$x^3 + y^3 + z^3 = 0,$$

which has already been considered. It follows from this equation that one of the unknowns must be divisible by 3; for otherwise each of them would be of the form $3n \pm 1$, and then their cubes would be of the form $27n^3 \pm 27n^2 + 9n \pm 1$, that is of the form $9m \pm 1$. But obviously the sum of three numbers each of the form $9m \pm 1$ cannot be zero, as this sum is not divisible by 9. Hence one of the unknowns must be divisible by 3.

Similarly it can be shown that one of the unknowns must be divisible by 7. For it is easily shown that the cubes of all numbers not divisible by 7 are of the form $7m \pm 1$, so that the sum of the cubes of three numbers cannot be divisible by 7, and hence certainly not equal to zero, unless one of the numbers is divisible by 7.

The question at once arises—Can an infinite number of primes q be found with the same property as the primes 3 and 7 above; that is to say, from the fact that $x^3 + y^3 + z^3$ is divisible by q, does it follow that one of the unknowns must be divisible by q? If so, the equation will be impossible, since one of the unknowns will be divisible by an infinite number of primes. A similar question suggests itself for the equation

$$x^p + y^p + z^p = 0.$$

Libri in 1832 stated without proof that an infinite number of primes such as q did not exist. This was proved by Pellet about 1886, and independently in 1909 by Dickson and Hurwitz amongst others. Dickson† also showed that

$$x^p + y^p + z^p$$

* Bachmann, *Niedere Zahlentheorie*, Vol. II. Chapter IX. will be found useful in connection with the first and third chapters of this book.

† *Crelle's Journal*, Vol. CXXXV. 1909, p. 181. Cf. also the paper by Hurwitz in Vol. CXXXVI. p. 272. A simple and elementary proof with rather larger limits for q

Hosted by Google

could be made divisible by q without any of the quantities x, y, z being divisible by q if

$$q \geqslant (p-1)^2(p-2)^2 + 6p - 2.$$

Hence the suggested method of attack cannot succeed in proving the truth of Fermat's Last Theorem.

Sophie Germain's result

Another line of attack depends upon some formulae discovered independently by a number of investigators, among whom may be mentioned Legendre, Abel and Peter Barlow, and developed by others such as Sophie Germain. It may be noted that Barlow was the first Englishman to write a treatise on the Theory of Numbers, and was also amongst the earliest writers who have given erroneous proofs of Fermat's Last Theorem.

Instead of $$x^p + y^p = z^p,$$

consider the more symmetrical form

$$x^p + y^p + z^p = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (8),$$

which can be written as

$$-z^p = (x+y)\left(\frac{x^p + y^p}{x+y}\right).$$

We note now* that either z is not divisible by p, in which case the two factors on the right-hand side are prime to each other, or that z is divisible by p, in which case the two factors have a common factor p of which the first power only is contained in

$$\frac{x^p + y^p}{x+y}.$$

It follows now from symmetry, that if x, y and z are all prime to p, then

$$y + z = a^p, \quad \frac{y^p + z^p}{y+z} = \xi^p, \quad x = -a\xi,$$

$$z + x = b^p, \quad \frac{z^p + x^p}{z+x} = \eta^p, \quad y = -b\eta,$$

$$x + y = c^p, \quad \frac{x^p + y^p}{x+y} = \zeta^p, \quad z = -c\zeta,$$

from which

$$2x = b^p + c^p - a^p, \quad 2y = c^p + a^p - b^p, \quad 2z = a^p + b^p - c^p.$$

(prime or composite) was given by Schur in the *Jahresber. d. Deutschen Math.-Vereinigung*, Vol. xxv. 1916.

* See p. 8.

Hosted by Google

CAMBRIDGE: PRINTED BY
J. B. PEACE, M.A.,
AT THE UNIVERSITY PRESS

Hosted by Google